



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,370	07/28/2004	Jaakko Rajaniemi	59643.00488	7601
32294	7590	03/27/2006		
SQUIRE, SANDERS & DEMPSEY L.L.P. 14TH FLOOR 8000 TOWERS CRESCENT TYSONS CORNER, VA 22182			EXAMINER LOFTIN, CELESTE	
			ART UNIT 2617	PAPER NUMBER

DATE MAILED: 03/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/500,370	HELSINKI, JAAKKO RAJANIEMI	
	Examiner	Art Unit	
	Celeste L. Loftin	2686	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 December 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 28 June 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 3,4,6-14,16-22,24, and 26-28 are rejected under 35 U.S.C. 102(b) as being anticipated by Chavez et al. (Chavez), **US Patent 6,591,102**.

Regarding claim 1, Chavez discloses a method for providing access to a service for a user in a communication system, comprising the steps of:

using a specific record, associated with said user, at a node in the communication system, containing information which, determines that a user is to be verified prior to providing access to said service (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information, (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 25-60, col. 1 lines 40-50**).

Regarding claim 3, Chavez discloses the method as claimed in claim 1 further comprising the steps of:

deciding based on said information that the authentication and/or authorization needs be verified (if the request is an incoming service request, base station reads the

Art Unit: 2686

authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information, (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 25-60, col. 1 lines 40-50**).

Regarding claim 4, Chavez discloses the method as claimed in claim 1 further comprising the steps of:

performing the authentication and/or authorization (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information, (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 25-60, col. 1 lines 40-50**).

Regarding claim 6, Chavez discloses the method as claimed in claim 4 further comprising the steps of:

performing the authentication and/or authorization in the node if the required parameters are available (if service information is not stored in the memory from a previous request for the service information, the MSC requests the service information from a service provider) (**col. 6 lines 20-35**).

Regarding claim 7, Chavez discloses a method for providing a user of user equipment with access to a service from a service provider node in a wireless communication system, comprising the steps of:

using a user specific record indicating a condition which, if satisfied, determines that a user characteristic is to be verified prior to providing access to said service (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 25-60, col. 1 lines 40-50**); and

providing access to said service responsive to said user specific record (after the base station requests authentication information the authentication process is carried out as normal) (**col. 5 lines 25-60**).

Regarding claim 8, Chavez discloses the method as claimed in claim 7 further comprising the steps of:

determining if said condition is satisfied (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 25-60, col. 1 lines 40-50**); and

providing access to said service without verifying said user characteristic if said condition is not satisfied (if the authentication information is stored then authorization takes place like normal and there is not need for a request for authentication information) (**col. 5 lines 25-60**).

Regarding claim 9, Chavez discloses the method as claimed in claim 7 further comprising the steps of:

determining if said condition is satisfied (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 25-60, col. 1 lines 40-50**);

verifying said user characteristic if said condition is satisfied (when an incoming service request is received the base station reads the authentication information and compares it to the authentication information stored in memory (the condition that is satisfied is that it is stored in memory)) (**col. 5 lines 25-60**); and

subsequent to said step of verifying the user characteristic providing access to said service if said user characteristic indicates the user is permitted access to said service (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it

isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 25-60, col. 1 lines 40-50**).

Regarding claim 10, Chavez discloses the method as claimed in claim 7 further comprising the steps of:

determining if said condition is satisfied when a call session between said user and said service provider node is initiated (if the request is an incoming service request (this could be a request for an outgoing service request including a telephone number requesting a call), base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 10-60, col. 1 lines 40-50**).

Regarding claim 11, Chavez discloses the method as claimed in claim 7 further comprising the steps of:

determining from the user specific record associated with said user if said condition exists during a call session between said user equipment and said service provider node (if the request is an incoming service request (this request could be an incoming service request form the MSC to provide a communication service to mobile handset), base station reads the authentication information from the incoming service

request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 25-60, col. 1 lines 40-50**).

Regarding claim 12, Chavez discloses the method as claimed in claim 7 wherein said wireless communication system comprises a serving network in which said user equipment is located, and a home network, said method further comprising the steps of:

indicating, via said user specific record, when access to said service is permitted without determining, from data stored at a node in said home network, if access is permitted (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 25-60, col. 1 lines 35-45**).

Regarding claim 13, Chavez discloses the method as claimed in claim 7 wherein said wireless communication system comprises a serving network in which said user equipment is located, and a home network (when a mobile enters a cell serviced by an antenna and transmits a location registration to the base station which transmits it to the MSC (there must be a home network and a serving network because the process is

executed every time the cell moves to a new cell, also the information is retained for future use)) (**col. 1 lines 35-65**), said method further comprising the step of:

storing said user specific record at a node of said serving network (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 25-60, col. 1 lines 35-45**).

Regarding claim 14, Chavez discloses the method as claimed in claim 7 further comprising the steps of:

generating a register message at said user equipment and transmitting said register message to a local server node of said communication system (if a the service information is not stored in memory from a previous request for the service information, a request is sent to the service provider which has a database that stores all the services a mobile is allowed to receive) (**col. 6 lines 20-35, col. 1 lines 35-60**);

determining if a condition indicated by said user specific record stored at said local server node is satisfied (the service provider then transmits the service information back to the MSC the MSC stores the information in memory) (**col. 6 lines 20-65**);

generating an access message at said local server node indicating that access to said service is permitted (service information is transmitted to the MSC which transmits

the information to the base station and then authentication takes place) (**col. 6 lines 20-65, col. 5 lines 25-60**); and

transmitting said access message to said service provider node (if the authentication is successful service is provided to the user) (**col. 6 lines 25-60**).

Regarding claim 16, Chavez discloses the method as claimed in claim 7 further comprising:

generating an invite message at said user equipment and transmitting said invite message to a local server node of said communication system (if a the service information is not stored in memory from a previous request for the service information, a request is sent to the service provider which has a database that stores all the services a mobile is allowed to receive) (**col. 6 lines 20-35, col. 1 lines 35-60**);

determining if a condition indicated by said user specific record stored at said local server node is satisfied (the service provider then transmits the service information back to the MSC the MSC stores the information in memory) (**col. 6 lines 20-65**);

generating an access message at said local server node indicating that access to said service is permitted (service information is transmitted to the MSC which transmits the information to the base station and then authentication takes place) (**col. 6 lines 20-65, col. 5 lines 25-60**); and

transmitting said access message to said service provider node (if the authentication is successful service is provided to the user) (**col. 5 lines 25-60**).

Regarding claim 17, Chavez discloses the method as claimed in claim 7 wherein said user characteristic comprises whether said user is authorized to access said

Art Unit: 2686

service (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) **(col. 5 lines 25-60, col. 1 lines 35-45).**

Regarding claim 18, Chavez discloses the method as claimed in claim 7 wherein said user characteristic comprises whether said user is authenticated to access said service (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) **(col. 5 lines 25-60, col. 1 lines 35-45).**

Regarding claim 19, Chavez discloses the method as claimed in claim 7 wherein said condition determines the frequency at which said user is to be authorized and/or authenticated during a call session between said user equipment and said service provider node (if the request is an incoming service request (this request could be an incoming service request form the MSC to provide a communication service to mobile handset), base station reads the authentication information from the incoming service

Art Unit: 2686

request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) **(col. 5 lines 25-60, col. 1 lines 40-50)**.

Regarding claim 20, Chavez discloses the method as claimed in claim 1 wherein said step of using a specific record comprises storing a user specific record (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) **(col. 5 lines 25-60, col. 1 lines 35-45)**).

Regarding claim 21, Chavez discloses a server node of a communication system for providing a user of user equipment with access to a service from a service provider node, said server node comprising:

means for receiving a message from said user equipment (the base station receives an incoming request for service from the handset) **(col. 5 lines 10-35)**;

means for using a user specific record, associated with said user, indicating a condition which, if satisfied, determines that a user characteristic is to be verified prior to providing said user with access to said a service (if the request is an incoming service

request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information, (the service provider maintains records as to which services that mobile handset) **(col. 5 lines 25-60, col. 1 lines 40-50)**.; and

means for generating, in response to said user specific record, an access message for providing said user with access to said service (if the authentication is successful service is provided to the user) **(col. 5 lines 25-60)**.

Regarding claim 22, Chavez discloses the server node as claimed in claim 21 further comprising:

means for transmitting said access message to a service provider node (if the service information is not sorted in the memory the MSC requests the information from the service provider) **(col. 6 lines 20-50)**.

Regarding claim 24, Chavez discloses a server node as claimed in claim 21 comprising a serving or proxy-call session control function node (if the service information is not sorted in the memory the MSC requests the information from the service provider) **(col. 6 lines 20-50)**.

Regarding claim 6, Chavez discloses the server node as claimed in claim 21 wherein said means for using a user specific record comprises means for storing (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base

station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 25-60, col. 1 lines 35-45**).

Regarding claim 27, Chavez discloses mobile user equipment, for providing a user with access to a service from a service provider node, comprising:

means for using a user specific record associated with said user, indicating a condition which, if satisfied, determines that a user characteristic is to be verified prior to providing said user with access to said a service (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 25-60, col. 1 lines 35-45**); and

means for generating, in response to said user specific record, an access message for providing said user with access to said service (if the authentication is successful service is provided to the user) (**col. 5 lines 25-60**).

Regarding claim 28, Chavez discloses mobile user equipment as claimed in claim 27 wherein said means for using a user specific record comprises means for storing a user specific record (if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information

Art Unit: 2686

may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information (meaning authentication information is not present and information is need for verification), (the service provider maintains records as to which services that mobile handset) (**col. 5 lines 25-60, col. 1 lines 35-45**).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 2,5,15,23, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chavez et al. (Chavez), **US Patent 6,591,102**, in view of, Basilier et al (Basilier), **US Patent 6,728,536**.

Regarding claim 2, Chavez discloses the method as claimed in claim 1 further comprising the steps of: but fails transferring said information from the AAA-H to the serving node in the signaling path for the service setup and/or service event and/or registration.

In a similar field of endeavor, Basilier discloses transferring said information from the AAA-H to the serving node in the signaling path for the service setup and/or service event and/or registration (the AAAF, AAAB, AAAH are on the same server so the AAB

transmits the application specific information to the application home server which validates or denies authentication) (**col. 6 lines 45-60, col. 4 lines 20-30**).

At the time of the invention it would have been obvious to one of ordinary skill in the art to modify Chavez to include transferring said information from the AAA-H to the serving node in the signaling path for the service setup and/or service event and/or registration. Motivation for this modification would have been to apply a protocol that the home and visiting networks can communicate with.

Regarding claim 5, Chavez discloses the method as claimed in claim 4, but fails to disclose further comprising the steps of: performing the authentication and/or authorization by using the AAA-H.

In a similar field of endeavor, Basilier discloses further comprising the steps of: performing the authentication and/or authorization by using the AAA-H (the AAAF, AAAB, AAAH are on the same server so the AAB transmits the application specific information to the application home server which validates or denies authentication) (**col. 6 lines 45-60, col. 4 lines 20-30**).

At the time of the invention it would have been obvious to one of ordinary skill in the art to modify Chavez to include further comprising the steps of: performing the authentication and/or authorization by using the AAA-H. Motivation for this modification would have been to apply a protocol that the home and visiting networks can communicate with.

Regarding claim 15, Chavez discloses the method as claimed in claim 14, but fails to disclose further comprising: prior to said step of storing said user specific record,

Art Unit: 2686

generating a request message at said local server node and transmitting said request message to the home AAA server of the user; and transferring data comprising said user specific record from said home AAA server to said local server node responsive to said request message.

In a similar field of endeavor, Basilier discloses prior to said step of storing said user specific record, generating a request message at said local server node and transmitting said request message to the home AAA server of the user; and transferring data comprising said user specific record from said home AAA server to said local server node responsive to said request message (the AAAF, AAAB, AAAH are on the same server so the AAB transmits the application specific information to the application home server which validates or denies authentication) (**col. 6 lines 45-60, col. 4 lines 20-30**).

At the time of the invention it would have been obvious to one of ordinary skill in the art to modify Chavez to include prior to said step of storing said user specific record, generating a request message at said local server node and transmitting said request message to the home AAA server of the user; and transferring data comprising said user specific record from said home AAA server to said local server node responsive to said request message. Motivation for this modification would have been to apply a protocol that the home and visiting networks can communicate with.

Regarding claim 23, Chavez discloses a server node as claimed in claim 21, but fails to disclose further comprising: means for receiving data comprising said user specific record transmitted from a home AAA server node.

In a similar field of endeavor, Basilier discloses means for receiving data comprising said user specific record transmitted from a home AAA server node (the AAAF, AAAB, AAAH are on the same server so the AAB transmits the application specific information to the application home server which validates or denies authentication) (**col. 6 lines 45-60, col. 4 lines 20-30**).

At the time of the invention it would have been obvious to one of ordinary skill in the art to modify Chavez to include means for receiving data comprising said user specific record transmitted from a home AAA server node. Motivation for this modification would have been to apply a protocol that the home and visiting networks can communicate with.

Regarding claim 25, Chavez discloses a server node as claimed in claim 21 but fails to disclose wherein said user specific record comprises a first data field identifying said user and a second data field determining when authentication and/or authorization of said user is required in order to access said service.

In a similar field of endeavor, Basilier discloses wherein said user specific record comprises a first data field identifying said user and a second data field determining when authentication and/or authorization of said user is required in order to access said service (the HLR stores information regarding features and services subscribed to by each user) (**col. 3 lines 35-50**).

At the time of the invention it would have been obvious to one of ordinary skill in the art to modify Chavez to include wherein said user specific record comprises a first data field identifying said user and a second data field determining when authentication

Art Unit: 2686

and/or authorization of said user is required in order to access said service. Motivation for this modification would have been to apply a protocol that the home and visiting networks can communicate with.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Celeste L. Loftin whose telephone number is 571-272-2842. The examiner can normally be reached on Monday thru Friday 8am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Marsha Banks-Harold can be reached on 571-272-7905. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CL


MARK CONTEE
EXAMINER